HOUSE . . . . . No. 213

The Commonwealth of Massachusetts

PETITION OF:

Michael A. Costello

In the Year Two Thousand and Seven.

AN ACT RELATIVE TO ENHANCING THE CONFIDENTIALITY AND PROTECTION OF CERTAIN CONSUMER INFORMATION.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1. The General Laws are hereby amended by inserting after chapter 66A the following chapter:--

Chapter 66B

Personal Data Protection

Section 1. As used in this chapter, the following words shall have the following meanings unless the context clearly requires otherwise:
(1) "Breach of the security of the system" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure;
(2) "Commercial entity" includes corporations, business trusts, estates, trusts, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities, or any other legal entity, whether for profit or not-for-profit;
(3) "Notice" means:

a. Written notice;
b. Telephonic notice;
c. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001 of Title 15 of the United States Code; or
d. Substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed $250,000, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that the individual or the commercial entity does not have sufficient contact information to provide notice. Substitute notice consists of all of the following:
1. E-mail notice if the individual or the commercial entity has e-mail addresses for the members of the affected class of Massachusetts residents; and
2. Conspicuous posting of the notice on the web site page of the individual or the commercial entity if the individual or the commercial entity maintains one; and
3. Notice to major statewide media.
(4) "Personal information" means a Massachusetts resident's first name or first initial and last name in combination with any 1 or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted:
a. Social Security number;
b. Driver's license number or Massachusetts Identification Card number; or
c. Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.
The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records;

Section 2.
Disclosure of breach of security of computerized personal information by an individual or a commercial entity.
(a) An individual or a commercial entity that conducts business in Massachusetts and that owns or licenses computerized data that includes personal information about a resident of Massachusetts shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about a Massachusetts resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible to the affected Massachusetts resident. Notice must be made in the most effective and expedient time possible and without

unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.
(b) An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach, if misuse of personal information about a Massachusetts resident occurred or is reasonably likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach.
(c) Notice required by this chapter may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by this chapter must be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.

Section 3.
(a) Under this chapter, an individual or a commercial entity that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notice requirements of this chapter if the individual or the commercial entity notifies affected Massachusetts residents in accordance with its policies in the event of a breach of security of the system.
(b) Under this chapter, an individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this chapter if the individual or the commercial entity notifies affected Massachusetts residents in accordance with the maintained procedures when a breach occurs. This chapter shall not apply to any financial institution, trust company or credit union that is required by the federal gram-Leach-Bliley Act of 1999, 15 U.S.C. s. 6801-6809 or any other state or federal statute, regulation or other regulatory action to notify consumers of a breach of security and is subject to examination by its functional governmental regulatory agency for compliance with applicable federal law.

Section 4:

Notwithstanding any other provision of law or contract and in addition to any other liability of a commercial entity to a bank as defined in section 1 of Chapter 167, whenever a commercial entity is required to provide notice to a consumer pursuant to section 3 of this act or to a bank pursuant to section 3 of this act, the

commercial entity shall be liable to such bank for the costs of reasonable actions undertaken by the bank on behalf of customers of the bank as a direct result of an actual breach of data security in order to protect sensitive financial personal information of such customer or to continue to provide financial services to any such customer, including any cost incurred as a result of a potential or actual breach of data security in connection with:

a) the cancellation or reissuance of any credit card issued by any bank as defined in Chapter 167, or access device as defined in section 1 of chapter 167B;
b) the closure of any deposit, transaction, share draft or other account and any action to stop payments or block transactions with respect to any such account;
c) the opening or reopening of any deposit, transaction, share draft, or other account for any customer of the bank;
d) any refund or credit made to any customer of the bank as a result of unauthorized transactions.

Section 5.

The Office of Consumer Affairs and Business Regulation is hereby authorized and directed to prescribe regulations necessary to implement this section within 6 months from the effective date of this act. Such regulations shall include a method of enforcing and collecting the costs owed to banks pursuant to this section.